IEEE P802.15

Wireless Personal Area Networks

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | May meeting for SG Privacy |
| Date Submitted | 18th May 2023 |
| Source | Tero Kivinen | E-mail: kivinen@iki.fi |
| Re: | May interm session |
| Abstract | Meeting minutes for the SG Privacy |
| Purpose | Provide meeting minutes |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend, or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

# IEEE SG Privacy

## **Tuesdays**, May **16th**, 2023

1. The SG chair Tero Kivinen called the meeting in order at 10:30 EST on Tuesdays, May 16th, 2023. Tero Kivinen made call for essential patents. No one had anything to disclose.

This session is a combination of two previously scheduled sessions into a single slot, and the agenda was approved after it was modifiedas shown on page 11 of doc#15-23-0251-01.

Openening slides were presented from doc#15-23-0251-01.

As there were quite a few 802.11 members in the meeting, Tero Kivinen started by giving background information by presenting 15-22/0477r00.

IEEE 802.15 hasn’t looked into privacy as much before because most devices weren’t mobile or connected to people. Now, however, IEEE 802.15.4 radios are being added to mobile devices that move with people – phones, remote controls, sensors (body/vehicle), trackers (luggage, etc.). And there is now a greater appreciation of possible attacks against these devices.

After the background information feedback from privacy experts was solicited to improve the list of issues, particularly as IEEE 802.11 participants have learned lessons during the development of IEEE 802.11bi and IEEE 802.11bh. The revised list is found in 15-23/0253r01.

After going through list of issues, Tero Kivinen went through the closing report (combined with the opening slides) in doc#15-23-0251-01.

It was agreed that it would be good idea to held similar combined meeting in July plenary, i.e., an attempt to coordinate a joint meeting during the July plenary beforehand.

The meeting was adjourned at 13:59 EST.

This is the discussion that happened during the meeting, it is not part of the official minutes, but is kept here as it is important points were made during this feedback.

C: You mentioned frame numbering (section 1.2.3). You have to be cautious with that. If all devices change the frame counter to zero at the same time and a whole bunch of new addresses show up, linking is hard. But if only one device shows up, it’s possible to correlate the old address with the new.

C: In 11bi, we don’t have an agreed solution, but I’m proposing to have multiple MAC addresses per device. That way, it’s hard to tell how many devices a user has. As long as the addresses are rotated frequently, correlation of a user with a device count becomes hard. Since we have groupcast addresses, IEEE 802.11 devices already support multiple addresses.

Q: Are frame numbers sequential or randomized?

A: Sequential. They are used for retransmission and replay detection.

C: With an omnipotent observer, when we change the MAC address, we have change things like the scrambler, sequence number, etc. But the observer will also have a sense of sequence numbers that have been used and not, so non-zero, randomized sequence numbers aren’t completely protective either.

C: The management of multiple addresses is tricky. Devices that wake up after a long while may have messages for you that use an old address that you have switched away from. It’s helpful to be able to know when you can fully deprecate an old address without causing an inability to receive data.

C: Almost all unicast frames are acknowledged. Retransmissions are done until a decision is taken to notify the upper layer that transmission failed. Wake up times can also be coordinated to reduce problems with reception. But many of the mechanisms that deal with low power will not deal well with privacy addressing. Transmission of ranging frames, if done frequently, can also make tracking of a device easier, even in the face of address changes. We are looking to solve problems for phones and body-carried sensors. Mostly, we won’t deal with industrial type networks because they aren’t so privacy sensitive, and they have attributes that make them easily tracked.

C: For ranging, the device MAC needs to change periodically (maybe not every round), but the fixed devices being ranged against don’t need to do that.

C: 802.15 devices don’t have certificates for identification of infrastructure elements like you would do on the Internet. So, ranging could be done with a random address every time as there is no identification or security context to be considered.

C: Consider drawing out the use cases that you want to protect against. Are you protecting against the observer? Do you want to make sure a shop doesn’t know you came back to them. Are you trying to make it harder for the observer to tell if one device has changed. Or do you want to make sure that a WPAN can be identified by an observer so that if one device is tracked, the rest of the devices can be tied to it.

C: Sometimes, it’s hard to tell what requirements the hardware vendors have. They seem to be proprietary.

C: There might be a need for a location-specific address. By choice, the user allows the device to be trackable in a shop in order to obtain discounts.

Q: I noticed you talked about the starting sequence number being zero every time. There was an attack on TCP based on the known sequence number.

A: Sequence numbers are only used to ack packets sent out and are tied to having a cryptographic key. Without the key, an attacker (not part of the group), would not be able to mount a sequence number-based attack. The sequence number could be reset to a random number. With frequent sequence number changes, there might not even be a rollover. But the frame counter is reset on rekey, which is a costly operation with asymmetric cryptography.

C: One other that comes to mind, if your sequence number rolls over at a count of 256, is there a concern that someone would do pattern recognition of 0xff or something like?

C: I don’t think there’s as much of an issue with the sequence number, which has a small value range. Acks of sequence numbers can be confusing because of hidden nodes, but enhanced sequence numbers help. Acks aren’t a guarantee that the upper layer received or dealt with a packet. They are only at the radio level.

Q: It would be helpful to understand better your use cases. How do group keys work? What’s the coordination?

A: IEEE 802.15.4 security is similar to Bluetooth security in many cases. Small number of connections at most, unlike IEEE 802.11 devices that might have many security setups. Other protocols and upper layers deal with setting up keys or security contexts.